Privacy

1. Purpose:

This policy concerns data privacy, confidentiality and security.

2. Policy:

The Maine Center for Disease Control and Prevention (Maine CDC) is committed to safeguard, protect and secure all individually identifiable health information entrusted to it in accordance with applicable state or federal law. The guiding principles for safeguarding individually identifiable public health data are that disclosures may only be made according to law and only the minimum amount of data necessary to protect public health and arrest potential disease contagion may be shared. Units of the Maine CDC subject to more restrictive criteria, via grant or mission specifications, regarding the use, administration, management, processing, storage, disclosure and sharing of individually identifiable health information gathered, furnished or developed by the Maine CDC shall abide by such restrictions.

3. Rationale:

The Maine CDC is charged with collecting a wide variety of health-related data. These data are obtained to fulfill our public health mandate, including but not limited to conducting: public health surveillance of diseases, other conditions and risk factors; epidemiologic studies; assessments of population health; investigation of unusual occurrence of diseases and/or environmental hazards or exposures; evaluation of programs and interventions; and compilation of vital statistics.

Many Maine CDC databases contain personal information about individuals. Release of directly or indirectly individually identifiable data, whether intentional or unintentional, could result in negative consequences, both for individuals about whom data are collected and the programs that collect and disseminate this information. Some possible negative consequences for individuals may include decline in property value, loss of job, legal prosecution, embarrassment, loss of health care, and threats of physical violence. Negative consequences for programs may include decreased ability to collect data, loss of public confidence and participation in the program, decreased ability to benefit the public, and threats of physical violence for service providers.

Despite risks associated with inappropriate data release, Maine CDC data are vitally important to maintaining the health of all people, and have wide and varied uses both within State government and in the larger public health community. Therefore, Maine CDC programs must make data available and accessible to the broadest possible constituency, while at the same time maintaining strict standards to protect individual privacy.

In addition, the implementation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) has engendered new awareness about the importance of data security and confidentiality among organizations that provide health-related services. HIPAA establishes federal requirements for the protection of personal health information, focusing primarily on information related to treatment, payment and other health care operations. Although most of the Maine CDC, as a public health entity, is exempt from most of these requirements, this Maine CDC policy strives to equal the confidentiality measures mandated by HIPAA, as well as regulations established in the American Recovery & Reinvestment Act of 2009.

4. Designation of Privacy Officer and Contact Office:

In order to centralize the management and administration of this policy, the Maine CDC has designated the agency's Privacy Officer. As such, the office of the Privacy Officer will be responsible for receiving complaints concerning the Privacy Policy; receiving complaints concerning Maine CDC confidentiality and data security compliance issues; ensuring ongoing staff training and compliance; updating the policy; and providing information regarding Maine CDC compliance with other related privacy and confidentiality regulations.

5. Classifying Restricted and Unrestricted Data:

Not all data collected and stored by the Maine CDC contain sensitive, individually identifiable information. Unidentified data or data not pertaining to health issues need not be protected with the same rigor or vigilance as more sensitive data that could be used to identify an individual. To clearly distinguish between sensitive and less sensitive information, this policy presents a classification scheme to be applied to all data sets collected and maintained by Maine CDC programs. The classification scheme aims to expedite data release and encourage release of the broadest spectrum of data elements without compromising confidentiality. Data are classified into two categories: restricted and unrestricted. Both types of data are subject to the rules related to cell size in Section 5.5.

5.1 Unrestricted Data

Unrestricted data contain no information that could be used directly or indirectly to identify individuals. Therefore, these data are to be made readily available for use both within the Maine CDC and by the general public.

5.2 Restricted Data

Restricted data include any and all information created or received by the Maine CDC that relates to: the past, present, or future physical or mental health or condition of an individual; the provision of health services to an individual; the past, present, or future payment for the provision of health services to an individual; or certain environmental, environmental health or toxicological data derived from individually-owned dwellings, land, or businesses; *and* that allows for the direct or indirect identification of that individual.

Identifiers that may be considered restricted include, but are not limited to, the following:

Name;
Date of birth;
Postal/residential address information;
Latitude and longitude of street address;
Telephone number;
Fax number;
Electronic mail (email) address;
Social security number;
Medical record number;
Health plan beneficiary number;
Account number; and
Vehicle identifier and serial number, including license plate number.

6. Data Release

For purposes of this policy, "data release" refers to provision of data to entities outside of the program where data are collected, stored and managed. This section describes methods for release of both restricted and unrestricted data.

Please note that some types of data are extremely sensitive and will be subject to more stringent restrictions for release and use than are described here. Units of the Maine CDC subject to more restrictive criteria regarding the use, administration, management, processing, storage, disclosure and sharing of individually identifiable health information gathered, furnished or developed by the Maine CDC shall abide by such restrictions. To the extent a unit of the Maine CDC is considered a covered entity within the meaning of the Health Insurance Portability and Accountability Act of 1996 (45 CFR Parts 160 and 164), the applicable standards, rules and regulations established under that statute are applicable to the particular unit of the Maine CDC.

6.1 Point of Contact

At least one individual shall be designated within each Division, preferably a data manager, to manage the release of both restricted and unrestricted data. This person should receive, review, respond and track each data request. In addition, data releases should be checked and verified by another qualified staff person (i.e. a staff person who is familiar with the program's data and has received both basic and more detailed training on this policy) prior to their release to ensure data confidentiality. Erroneously released data could lead to a breach of confidentiality.

6.2 Release of Unrestricted Data

Many individual requests for unrestricted data can be satisfied through use of existing reports and publications produced by the Maine CDC, and may be freely released to the public.

Requests for unrestricted data not otherwise published may be made by telephone or in writing. Requests should be as specific as possible and, at minimum, must stipulate the data items requested, time period for the data, and a time frame for receiving the data. Requests must also clearly identify a contact person to whom the Maine CDC can respond. It is recommended, but not required, that requests for unrestricted data be logged electronically or in a paper file. See Model Document 1 (Attachment 1) for an example of an Application for Release of Unrestricted Data request form. (*Please note*: unrestricted data must be provided even if the requestor refuses to identify him or herself.)

6.3 Release of Restricted Data

Although Maine CDC data are vitally important for promoting and maintaining public health, inappropriate release of directly or indirectly identifiable data could result in harm both to individual Maine citizens and to Maine CDC programs. For this reason, it is crucial that Maine CDC employees and contractors strictly adhere to this Policy. Failure to do so could result in sanctions against the employee (see Section 10.2.)

In order to guide practice for data release, the terms "Internal," "Federal Partners," and "External" are used in this document to categorize the end-users of restricted data.

- "Internal" users are Maine CDC employees, including non-State contracted workers employed within Maine CDC programs and supervised by Maine CDC staff. Internal users also include outside agencies (such as MaineCare and ChildLINK) and outside providers (such as Maine Breast and Cervical Health Program providers) with whom data sharing is necessary to carry out Maine CDC operations. In addition, an outside entity *may* be considered an Internal user in the following circumstances: the entity's primary mission is public health; the entity has demonstrated competence in epidemiology, data security, and confidentiality; and the entity has a demonstrated need to know the information requested. Please note that data sharing with programs and providers outside of the Maine CDC requires a contract, memorandum of understanding (MOU), Trading Partner Agreement, Client Consent Statement, or other written agreement that holds the organization/individual accountable to this policy.
- "Federal Partners" are federal government agencies, such as the US Centers for Disease Control and Prevention (CDC) and the US Health Resources and Service Administration (HRSA.)
- "External" users include users of restricted data who do not fall into the above categories.

Methods used to release restricted data differ depending on the category of the person or entity requesting data. These methods are described below.

6.3.1. Release of Restricted Data to Internal Users

As Maine CDC employees, Internal users share the Maine CDC mission to provide the leadership, expertise, information and tools to assure conditions in which all Maine people can be healthy. In addition, internal users are bound by

the strict confidentiality and security guidelines found both in this Maine CDC Privacy Policy and in related DHHS policies. For these reasons, this Privacy Policy allows Internal users broader access to restricted data than is permitted for External users.

To facilitate data sharing among Internal users, each program will contribute to a master *Data Inventory* and a master *Data Use Plan*. The Data Inventory and Data Use Plan will be used at the Maine CDC-wide level to assure that public health data are treated as an asset and utilized to the fullest extent. In addition, both the Plan and Inventory will be used to assure appropriate management and confidentiality of the data, and to assure that all users maintain the integrity of program data. The Plan and Inventory will be compiled and stored in the office of the Privacy Officer, with oversight by the Maine CDC Data Work Group. More detailed descriptions of the Plan and Inventory are included below.

6.3.1.a. Data Use Plan

The Maine CDC Data Use Plan will describe the Maine CDC's plan for data sharing with other Maine CDC programs, and will reflect the Maine CDC's vision and priorities for use and collection of public health information. Annually, each program will fill out the *Data Use* form (Attachment 7) to document data relationships between programs. This plan will detail the names of programs, types of data shared, frequency of use, and purpose of use. For each program, the Plan will incorporate all data used that is collected and stored in other programs, including data used for program planning and evaluation, epidemiology, case investigation, outbreak management, emergency response, and management/administration.

Once established, restricted data will only be released to appropriate Internal users as defined by the current Data Use Plan. Once included in the Data Use Plan, programs may share restricted data on an ongoing basis without additional approval. As new areas for data sharing are identified, the requesting program will submit a written request to the program of interest (see page 18 for Application for Release of Restricted Data.)

The Plan will be overseen by the Privacy Officer, with assistance from the Maine CDC Data Work Group. Program and division directors will facilitate data-sharing requests, with assistance from the Privacy Officer as appropriate.

6.3.1.b. Data Inventory

The Maine CDC Data Inventory will catalogue all data collected by Maine CDC programs, creating a Maine CDC-wide inventory of

public health data routinely collected, which may be viewed by potential Internal and External users.

A Data Inventory Form (Attachment 6) will be completed annually for all data sources collected by each program, whether paper or electronic. For each data source, the inventory will summarize the nature of the data (i.e. surveillance, service data, etc.,) how it is stored, description of the data collected, and type of routine summary reports that are available.

The Inventory will be overseen by the office of the Privacy Officer, with assistance from the Maine CDC Data Work Group.

6.3.1.c. Additional Restrictions

To the extent a unit of the Maine CDC is considered a covered entity within the meaning of the Health Insurance Portability and Accountability Act of 1996, the applicable standards, rules and regulations established under that statute are applicable to the data collected by that particular Maine CDC unit.

Some requests for restricted data require a research protocol and proof of approval by, or exemption from, an Institutional Review Board (IRB) formed and maintained in accordance with the U.S. Department of Health and Human Services Code of Federal Regulations for Protection of Human Subjects (45 CFR 46, revised March 8, 1983). Research projects require IRB approval before any data are released. For more information about the IRB and IRB requirements, see: http://www.maine.gov/dhhs/boh/IRB/irb08.htm

6.3.2 Release of Restricted Data to External Users

Restricted data will only be released to External users after the Maine CDC program designee(s) responsible for managing data requests has reviewed the request. The request must include an Application for Release of Restricted Data (see example, Attachment 2: Model Document 2) along with the Data Use Agreement (Attachment 3) and a research protocol and proof of approval by, or exemption from, an Institutional Review Board formed and maintained as noted above.

To the extent that a unit of the Maine CDC is considered a covered entity within the meaning of the Health Insurance Portability and Accountability Act of 1996, the applicable standards, rules and regulations established under that statute are applicable to the data collected by that particular Maine CDC unit.

If it is determined that part or all of a data request can be accomplished through in-house analysis, use of unrestricted data, or the creation of proxy variables,

the Maine CDC reserves the right to create such products to fill a request, rather than release the restricted data.

6.3.3 Release of Restricted Data to Federal Partners

Release of restricted data to federal agencies shall occur on an as-needed basis, with such release negotiated individually by Maine CDC programs. In most instances, agencies such as the U.S. CDC and HRSA are not routinely provided with individually identifiable data, although other restricted data elements, such as date of birth and demographic data for individuals, may be provided.

Federal agencies may occasionally assist Maine CDC personnel with disease outbreaks, epidemiologic investigations or events related to bioterrorism prevention and response. It is appropriate to share restricted data under these circumstances.

Consistent with data release practices discussed in other sections of this policy, the minimum amount of restricted data should be released to adequately perform a given public health function. In some instances, data requests from federal partners may need to be made in writing. It may also be appropriate to request that staff of federal agencies complete confidentiality forms.

6.4 Secondary Data Release

Secondary data are defined as "data received from another source within the Maine CDC." Often times, a program within the Maine CDC will publish or be asked to share data provided by another program within the Maine CDC.

The release of unrestricted secondary data should be made according to this Policy, including cell size, to ensure confidentiality. Before releasing secondary data collected and maintained by another program, the user should request verification from the person directly responsible for managing the data set in question. If this is not possible, verification shall be performed by an individual familiar with data quality and release, preferably an epidemiologist or program manager/director.

The release of restricted secondary data to programs within the Maine CDC or to outside entities is only allowed by an executed Memorandum of Understanding or Data Sharing Agreement. Requests for such data should be referred to the manager of the program where the restricted data originated. The request will then be processed according to the program's policy.

6.5 Cell Size

"Cells" refer to the space formed by the intersection of a row and column in a data table. For example, a data table may include the category "race" in columns and the category "county" in rows. The resulting cells within the table describe a population by

race and county. In some instances, cells provide very specific information about a limited number of people. In general, problems with confidentiality and privacy occur when there are small denominators, or population sizes, within a given cell in the table.

In order to reduce the risk of breaching confidentiality, the following guidelines shall be followed when releasing data:

- County level data will be released, regardless of the numerator cell size, if the underlying population of the cell is 5,000 or greater. ("Underlying population" refers to the total subpopulation described by the data, i.e. 15-24 year-old males.) A decision may be made to suppress county level data regardless of underlying population size if circumstances are such that there are reasonable concerns that release of the data could violate an individual's privacy or allow someone to identify an individual.
- County level data with cell sizes of 5 or fewer will be suppressed if the underlying population of the cell is less than 5,000.
- For geographic areas smaller than the county, regardless of the underlying population size, cell sizes of 5 or fewer will be suppressed.
- State level data will be released, regardless of numerator or denominator size. A decision may be made to suppress state level data if circumstances are such that there are reasonable concerns that release of the data could violate an individual's privacy or allow someone to identify an individual.

There are two primary methods used to release data that include small cell sizes: aggregation and suppression. These methods are described below.

Aggregation: Aggregating data is the primary method used to collapse a dataset in order to create tables with no small numbers as denominators or numerators in cells. Aggregation of data values is appropriate for fields with large numbers of values, such as dates, diagnoses, and geographic areas.

Suppression: When it is not possible or desirable to create a table where all cell sizes are greater than 5, cell suppression is used. Suppressed data will be reflected in tables as "five or fewer," "<5," "fewer than 6" or "<6." The method of "primary cell suppression" is used to withhold the numerator in the cell that does not meet the threshold. In the event that one cell is too small, two other "complementary" cells also need to be suppressed, including the next-larger cell and the total. This rule applies to both rows and columns whenever totals are presented. Complementary cell suppression must be completed in order to avoid inadvertent disclosure through back-calculation. Note that cell suppression is a method of last resort due to the amount of labor needed to ensure that confidential information is not accidentally released as a consequence of complementary suppression.

In the event of a public health emergency, where specific information is vital for public safety, release of confidential information will be at the discretion of the Maine CDC Privacy Officer.

6.6 Mapped Data

Geocoding is the process of assigning geographic identifiers (e.g., town/region codes or geographic coordinates expressed as latitude-longitude) to data records, such as those containing street addresses. When the geocoded coordinates of a health event are depicted as points on a map, it is possible to reveal an individual's confidential street address through a process of reverse geocoding. In order to protect confidentiality, a geographic masking approach must be used when publicly presenting restricted point-mapped data. Geographic masking is the process of modifying the geographic coordinates in order to mask the precise location of individual cases. Masking techniques include, but are not limited to, the following:

1. Data Aggregation: This technique involves aggregating individual data points into a larger geographical area, such as a census tract, zip code, county, or political boundary. Aggregation of data points must meet the guidelines for Cell Suppression in Section 6.5

2. Random Spatial Perturbation: This technique involves displacing each data point by a small, random distance in a randomly determined direction. Guidelines for applying random perturbation can be found in Chapter 8 of the book *Geocoding Health Data: The Use of Geographic Codes in Cancer Prevention and Control, Research, and Practice*, CRC Press, 2008, ISBN 978-0-8493-8419-6.

Methods of geographic masking may limit the usefulness of the data for investigating disease clusters and add complexity to the analysis. For this reason, these techniques are only recommended when presenting data publicly. The following journal article is also a source on masking techniques: Armstrong MP, Rushton G, Zimmerman DL: Geographically masking health data to preserve confidentiality. *Statistics in Medicine* 1999, 18:929-947.

7. Transmission of Restricted Data

When transmitting restricted data, a common-sense approach should be taken to ensure that only essential restricted data are shared in order to perform a required function. If possible and feasible, non-essential identifiers shall be removed when transmitting restricted data by U.S. mail, private mail carriers, facsimile or electronic mail.

All restricted data sent through U.S., private mail carriers, or interoffice mail shall be placed in envelopes stamped "Confidential." This applies to all mail containing restricted data. Ensure that the correct address is used, and that the address names an individual to receive the mail.

Restricted data transported between staff offices shall be placed in envelopes marked "confidential." All incoming restricted data shall be dated and appropriately distributed to program staff. At the end of each day, all materials with restricted data must be appropriately stored (see Section 9.)

Restricted public health data that are transmitted electronically should be 1) limited to those situations that require immediate receipt of the data; and 2) must be safeguarded against interception or access by persons who do not have clearance to view or use them.

Use of email and cell phones to transmit/discuss restricted data is allowed only under limited circumstances. Pursuant to the DHHS Policy Concerning Use of State Automation Equipment (Section IV, A):

> DHHS employees are hereby made aware that cell phones and Internet messages are generally not secure and can be easily intercepted by outside parties . . . Non-crypted cell phones and unsecured/non-encrypted Internet connections must not be used to discuss or disclose confidential or personal/protected health information (such as HIV status, substance abuse/treatment, mental health condition(s), etc.).

Cell phones issued by Maine CDC are encrypted. Restricted data may be discussed using encrypted cell phones when necessary to perform required job duties, and the person utilizing the encrypted cell phone has made a reasonable effort to conduct the phone call in a private setting where restricted information cannot be overheard.

At this time, email encryption is not available to Maine CDC personnel. Therefore, restricted data may not be emailed to non-state email addresses. Restricted data may be emailed only between State employees in password-protected documents and when the password has been conveyed to the receiver by other means.

Pursuant to Section IV, E of the DHHS Policy Concerning the Use of State Automation Equipment, all email messages containing password-protected restricted data must have a label placed in the subject line that reads: "Confidential Information Enclosed" (see section 6.1.)

When electronically transmitting restricted data, senders must ensure that a correct, updated email address or fax number is used. The sender must also verify that the data were received by obtaining from the receiver a voice, email or fax confirmation. If the data were not received, the sender must work with the State's Office of Information Technology (OIT) staff to determine the destination of the data and retrieve them if possible.

Fax machines used to transmit restricted data should be located in low traffic areas or secured locations, such as a locked room. The sending or receiving of faxes containing restricted information must be coordinated with the sender/receiver so that each is handled in a timely manner with little or no opportunity for other persons to view these data. Fax machines not located in a locked room should be disabled from printing when office hours are concluded.

7.1 Confidentiality Notice

Because of the potential for unintended receipt, all restricted data transmitted by fax or email shall contain the following confidentiality notice:

> ***Confidentiality Notice:*** This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. If you are not the intended recipient, or an authorized agent of the intended recipient, please immediately contact the sender by reply email or fax and destroy/delete all copies of the original message. Any unauthorized review, use, copying, disclosure, or distribution by other than the intended recipient or authorized agent is prohibited.

This notice must be placed at the bottom of a fax cover page, or as an email footer.

8. Employee Practices

8.1 Confidentiality Rules and Statement

All new employees shall be required to read and sign the DHHS Employees' Confidentiality Statement (Attachment 4), of which they will be given a copy. The original document shall be stored in the employee file. Signing this statement indicates that the employee understands the need to maintain client confidentiality and is aware of the penalties for failing to do so.

8.2 Employee Training

All Maine CDC employees must read this Policy and receive training about its content. Periodic privacy training will be offered to all Maine CDC employees. Ensuring that all employees are trained is the responsibility of each program director/manager.

Two training topics are recommended: a "basic training" and a more specific and detailed training for data managers.

Basic training should carefully review this Policy, with a focus on employee responsibilities and worksite security. Unless a Maine CDC-wide basic training is offered, program directors/managers or their designee(s) shall implement the training, which must be offered to all staff annually, and to new staff upon hire. Former employees re-hired by the Maine CDC shall be considered new employees in regard to training. Basic training may also include any additional standards and practices specific to divisions or programs. A sample basic training presentation in MS PowerPoint format is available for viewing by contacting the Privacy Officer.

Data manager training is mandatory for all Maine CDC data managers and Maine CDC employees authorized to perform data release to internal, external or federal partners. The training will focus on data release and cell size, use of data request forms, secondary data release, the Data Use Plan, and the Data Inventory. Data manager training will be periodically offered through the office of the Privacy Officer.

As needed, additional training will be provided to all staff following any substantial change made to this Policy.

8.3 Employee Access to Restricted Data

Access to restricted data shall be limited to those staff that collect, process or analyze the data on a program-specific level. Every effort shall be made to minimize the number of staff required to handle restricted data, with access granted on a "need-to-know" basis.

Data managers shall conduct periodic audits of their data systems to ensure that users are accessing restricted data appropriately. Suspected inappropriate access or use of restricted data must be reported as a potential breach following the protocols in section 10.1.1.

Maine CDC employees, including contracted workers employed within Maine CDC programs and supervised by Maine CDC staff, with access to restricted data may only access restricted data (via saved files or other applications) when working remotely in the following circumstances:

1. It is necessary to access the restricted data in that time and setting, and
2. The employee is using a State-issued laptop computer.

Pursuant to the DHHS Policy Concerning Use of State Automation Equipment (Section IV, E, 9):

If an employee uses a personal computer that is not provided by the Department, for State business purposes, the PC must have installed and operating the current version of the State-approved anti-virus product. The personal computer **must not** be used to access, download or store PHI or other confidential information.

8.4 Departing Employees

Staff who end Maine CDC employment or who change employment to another Maine CDC program shall, by their last scheduled working day, return all keys, including keys to offices, filing cabinets and storage areas. The employee will also return pass cards, identification cards, and issued equipment, such as laptop computers, personal digital assistants, Blackberrys and cell phones. In addition, the supervisor of the departing staff will discuss the need to adhere to the Confidentiality and Rules Statement, specifically that these rules extend beyond employment with any Maine CDC unit and that confidentiality must continue to be maintained even after employment with a Maine CDC unit is ended. These activities would typically occur as a part of a staff "exit interview," conducted by supervisors for departing staff. A record of this interview must be maintained for three (3) years.

9. Work Site Security

Restricted data must not be discussed in public areas.

Program staff shall be individually responsible for protecting their own work station. This responsibility includes protecting keys, passwords, and codes that would allow access to restricted information.

Visitors to Maine CDC offices must be accompanied at all times after being admitted to the office space. (In specific areas of Maine CDC it may be required that program staff be notified in advance that a visitor will be escorted to their space, allowing time for removal of confidential documents from workspaces, if necessary. Maine CDC staff will walk visitors out to the reception area when the visitor departs.)

If non-staff persons enter a work area containing restricted information, such data will be immediately removed from view (e.g. clearing computer screens, placing documents in desk drawer.) As appropriate, visitors should be escorted out of areas containing restricted data, and assisted in locating appropriate Maine CDC staff or offices.

All file cabinets containing confidential records are to be locked when not in use. Staff shall be responsible for making certain that file cabinets are locked within their workspace before leaving the office each day.

When staff are not present in offices for short periods (less than 30 minutes), databases containing restricted data must be closed so they will require use of a password to reopen. In addition, all confidential data shall be turned face down on desks and office surfaces. When staff depart for periods of 30 minutes or more, all confidential records shall be returned to their locked storage location. Staff that utilize restricted data throughout the workday will be located in low-traffic areas and will appropriately store materials with restricted data when away from the workstation for 30 minutes or more. All restricted data will be placed in a locked storage location when office hours are concluded.

10. Storage of Restricted Data

10.1 Written Records

At a minimum, written records containing restricted client data shall be stored in locked file cabinets. As practical, office spaces should be locked and alarmed when unoccupied.

If more than one person has access to written data, a single staff person will be designated as responsible for "signing out" restricted records used by other staff. This individual will be notified by other staff whenever confidential files are removed from their locked storage area. Preferably, the designee will track files through a written checklist or tally. In the case where an entire program requires access to written records with restricted data, staff will be individually responsible for returning records to file cabinets, or temporarily storing records or any material with restricted data in a locked storage area when office hours are concluded.

Data should be transported off site only when absolutely necessary. Staff who need to transport restricted written or electronic data outside the office must take extra care to safeguard these data, and should make every effort to restore data to the locked

storage location upon return to the program office. When possible, data should be transported in locked briefcases or lockable file carriers.

Written records determined to be non-essential by program staff (i.e. records entered into a computer database, phone messages, computer-generated line lists) shall be shredded after use.

10.2 Electronic Records

At minimum, electronic records containing restricted client data shall be stored either on removable computer devices, (which are then treated in the same way as written records) or on password-protected computers stored in locked and alarmed offices. As appropriate, data should be encrypted using 128-bit or higher encryption software, with access limited to those working directly with the data. For shared computer programs on a local area network (LAN,) data files will be password protected, with user rights limited to those staff who work directly to collect, enter or analyze these data. LAN backup files shall be treated in the same way as written data.

The OIT Policy to Safeguard Information on Portable Computer and Storage Devices states that restricted data must be safeguarded "by properly classifying data, using encryption to prevent unauthorized access, and requiring written authority to copy data to portable devices" (Section I). Examples of portable computer and storage devices include laptops, pocket personal computers, Blackberries, hand-held devices (PDAs), USB thumb drives, cell phones etc.

When practicable, data stored on a portable device (such as an encrypted USB drive) should be copies of data stored on a secure State network drive. The user assumes the responsibility for any original data stored on a portable, encrypted device when the device itself or password is lost.

10.3 Replacing Computer Equipment

When replacing computer hardware, any equipment used for storing restricted electronic records must be thoroughly purged of data before being removed from program offices. Purges must be conducted by qualified OIT staff who completely remove data so that it is "unrecoverable." In addition, removable storage devices no longer used to store restricted data must be either purged or destroyed by qualified OIT staff.

Program managers must inform OIT staff when any equipment being replaced had been used to store restricted electronic data. OIT staff is responsible for ensuring that purges are completed as appropriate.

11. Security Breach

11.1 Mandatory Reporting

Any Maine CDC employee who suspects wrongful or negligent release of identifiable or potentially identifiable data shall immediately report this information to his or her direct supervisor, who will then immediately notify their respective division director, the deputy director and the Privacy Officer.

Any violation of this Privacy Policy should immediately be brought to the attention of an employee's direct supervisor, who will then notify their respective division director, the deputy director and the Privacy Officer, even in the absence of an actual security breach. In addition, Maine CDC employees will report any other information, incidents, etc., as required by law or other policies and procedures, as established by the Maine CDC or the Department of Health and Human Services, to their direct supervisor, who will then immediately make the appropriate notifications.

11.1.1 Protocols for Reporting Suspected Breaches

Any suspected wrongful or negligent release of identifiable or potentially identifiable data, any violation of the Privacy Policy, or other reportable incident described above shall be reported to the appropriate division director(s), deputy director and the Privacy Officer by submitting an e-mail report detailing the date and nature of the suspected breach, a description of the identified information, the parties involved in the suspected breach, and any other relevant information. No personally identifying information need be included in this initial report.

All suspected breaches will be investigated by the Privacy Officer or his or her designee(s), who shall submit a detailed report of findings to the supervisor, division director(s), deputy director and other parties as necessary and appropriate.

11.1.2 Individual Breaches

This policy follows the definition of breach outlined in the American Recovery and Reinvestment Act of 2009 (P.L. 111-5): "the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information."

The following are not considered breaches for the purposes of this Policy:

- Unintentional acquisition, access, or use of protected health information when such action was made in good faith and within the scope of the employee's job functions, and when the information is not further acquired, accessed, used, or disclosed.

- Inadvertent disclosure from an individual who is authorized to access protected health information to a similarly situated staff member within the same program.
- Information received as a result of an inappropriate disclosure that is not further acquired, accessed, used, or disclosed without authorization.

When the Privacy Officer or his or her designee(s) determines that a breach has occurred, a log of the breach shall be created that includes a description of what happened, including the date of the breach and the date of discovery of the breach; and a description of the types of information that were involved in the breach. The Privacy Officer or his or her designee(s) will submit a final report to division director and deputy director describing how the breach was discovered and investigated and, as appropriate, strategies for preventing future breaches.

As required by the American Recovery and Reinvestment Act, Maine CDC programs deemed "covered entities" must provide individual notice of breaches within 60 calendar days of discovery of the breach, and an annual log of breaches to the U.S. Department of Health and Human Services. Individual notice must be delivered via first class mail, unless the individual has specified a preference to receive notices by electronic mail.

As appropriate, other programs not deemed to be covered entities shall provide individual notice of breaches by the same standards and reported as outlined above.

11.1.3 Multiple Breaches

In the case that the protected health information of multiple individuals is breached, the following notification standards apply for Maine CDC programs deemed to be covered entities:

- Individual written notice must be provided within 60 calendar days of discovery of the breach via first class mail, unless the individual has specified a preference to receive notices by electronic mail;
- If 10 or more individuals have insufficient or outdated contact information, a conspicuous posting shall be placed on the Maine CDC web page, including a toll-free phone number where an individual can learn whether or not the individual's information has been breached;
- If more than 500 individuals' protected health information is breached, notice shall be made to prominent media outlets, including a toll-free phone number where individuals can learn whether or not their information has been breached. Such breaches shall be immediately reported to the U.S. Department of Health and Human Services.

As appropriate, other programs not deemed to be covered entities shall provide notice of breaches by the same standards and in consultation with the Privacy Officer.

11.2 Sanctions

Upon notification of a Privacy Policy violation, the direct supervisor in coordination with the Privacy Officer, will investigate the alleged violation with the accused Maine CDC employee. The principles of progressive discipline will be followed, as dictated by the State's Bargaining Contracts. In the course of the investigation, disciplinary actions may include any of the following, depending on the severity of the security breach: oral reprimand, written reprimand, suspension, demotion and dismissal.

11.3 Whistle-Blower Exception

There will be no retribution or retaliation against employees for reporting violations, so long as reporting is done in good faith. Maine CDC management or staff will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against employees, business associates, et al, who either report violations to this Policy or who assist in investigations or other proceedings in relation to an alleged violation.

However, any employee who deliberately makes a false accusation with the purpose of harming or causing retaliation against another employee or the Maine CDC will be subject to disciplinary action.

11.4 Mitigation

Maine CDC will mitigate, to the extent possible, any harmful effect resulting from a breach of this Privacy Policy by an employee or other data user regarding release of restricted data. The Maine CDC will take reasonable steps to determine how restricted information was improperly disclosed, how it might be used to cause harm and what steps can be taken to alleviate the effect that resulted from the breach.

12. Documentation

The Maine CDC will maintain and keep up to date the Privacy Policy and associated procedures either on paper or in electronic form. All documentation will be maintained for six (6) years or in accordance with State of Maine record retention policies.

13. Notice of Privacy Practices

As required by HIPAA, Maine CDC programs deemed "covered entities" must provide a Notice of Privacy Practices to their clients (See Attachment 5, Model Document 3: Maine CDC Summary Notice of Privacy Practices). As appropriate, Maine CDC program participants or community stakeholders will be provided with adequate notice of any uses and disclosures of their health data that may be made. Specific Maine CDC Privacy Practices will be listed on the notice. The notice will be written in easy to read language, with

a simplified summary cover sheet explaining the key points. The notice will be made available in whatever language(s) the Commissioner of the Department of Health and Human Services, or their designee, deems appropriate.

14. Revision

The Privacy Officer is responsible for revising the Privacy Policy and procedures dealing with compliance as necessary. The Privacy Officer will ensure that affected policies and procedures are promptly revised as necessary, and appropriate notices are updated to reflect changes.

15. Denial of Access

If a request for data is denied, the applicant may appeal in writing to the Privacy Officer. If this appeal is also denied, appeal may then be made to the DHHS Hearings Unit. (Maine CDC Programs that fall under the HIPAA definition of "covered entity" may also be appealed to the Secretary of Health and Human Services.)

Privacy

Section #	Description of Change	Revision Approver	Approval Date
6.5	Clarification of data suppression		8/9/12

Attachment 1

Model Document 1: Application for Release of Unrestricted Data

Maine Center for Disease Control and Prevention
Department of Health and Human Services

1. Data Requestor

   Name _____

   Title _____

   Organization _____

   Address _____

   Email Address _____

2. Contact person:
   Name _____

   Telephone No. _____ FAX No. _____

3. Request made by: _____ telephone
   _____ writing

4. Purpose of how data will be used _____

   _____

5. Type of data requested: _____

6. Time period for data requested: _____

7. Time frame for receiving data: _____

8. Form of records requested:
   ____ Photocopies
   ____ Computer listing
   ____ Electronic file format; specifications: _____
   _____
   ____ Other - specify: _____

Maine CDC Program use only

Date received _____
By _____
Approved _____Yes _____No

Date of Approval Decision _____

Continuing request? _____
Approval valid until _____
Cost estimate (if applicable) $_____

Attachment 2
Model Document 2: Application for Release of Restricted Data

Maine Center for Disease Control and Prevention
Department of Health and Human Services

Title of Program and Data Set: _____

1. Principal Investigator or Program Director:

   Name _____

   Title _____

   Organization _____

   Address _____

   Email Address _____

2. User Category:
   _____Researcher
   _____Federal governmental worker
   _____State governmental worker
   _____Local governmental worker

3. Contact person:
   Name _____

   Telephone No. _____ FAX No. _____

4. Intended use of restricted data : _____Statistical research for medical, health or social services
   _____ Research Protocol
   _____ Proof of IRB approval or exemption
   _____ Public health planning, assessment or evaluation
   _____ Health services planning
   _____ Administrative reporting to state funding sources
   _____ Administrative reporting to federal funding sources
   _____ Other (be specific:_____)

5. Type of records requested: _____

6. Form of records requested:
   ____ Photocopies - certified
   ____ Computer listing
   ____ Electronic file format, specify: _____
   _____
   ____ Other - specify: _____

Maine CDC Program use only:

Date received: _____ Continuing request? _____
By:_____ Approval valid until _____

Approved _____Yes _____No Cost estimate (if applicable) $_____
Date of Approval Decision _____

Page 2: Supplemental Information:

1. **Will you supply identifying information to be used to select the records of interest?**

   ____ Yes ____ No
   If YES, what information?

   If NO, how is the general group of records you are requesting to be selected?

2. **Approximate number of records requested: _____**

3. **If your request calls for the release of data on an ongoing basis, how often will you need the data supplied, and over how long a period of time?**

4. **Summary of study/program protocol. Please be as succinct as possible; your complete study protocol or program and detailed descriptions of your project and background are not necessary.**

   a. Description of health or medical problem addressed or administrative purpose served by the program, demonstrating that data requested are essential, and stating primary study or program objectives and hypotheses to be tested, if applicable.

   b. Methodology; include justification for contact with individuals named on records/data and attach copies of contact letters and consent forms if applicable.

   c. Description of any data files that will be linked with the records/data, demonstrating that such linkage is essential for the stated purpose.

   d. Analysis plan, if applicable, indicating how data will be used and level of aggregation.

   e. Description of whether, and if so, to whom restricted data will be released, demonstrating that such release is related to stated purpose.

   f. Procedures for maintaining confidentiality and security of restricted data received on or through the use of records/data.

   g. Procedures and timetable for disposition of any records/data received.

5. **Attach copy of *Data Use Agreement*, signed by the Principal Investigator, Program Director, or other individual responsible for conformance to standards for release of restricted data.**

Attachment 3

Data Use Agreement

Maine Center for Disease Control and Prevention
Department of Health and Human Services

Data Use Agreement

I agree that the restricted data will not be used in a manner which will identify any individual in any results, presentations, or reports produced by the investigation, study or project, or for administrative purposes other than those specified in this application; that data released for statistical research use will not be used for administrative, legal or other non-statistical purposes which may directly affect particular individuals as a result of their identification in the study; that data/records will be aggregated in a manner that will protect the confidentiality of individuals, as stipulated in the Maine CDC Privacy Policy; and that disposition of restricted data will be made in a manner that will not permit unauthorized disclosure.

As the official or principal investigator of the program or research study named on this application which involves the use of Maine CDC restricted data, I agree to abide by the provisions of this *Data Use Agreement*. I will take all steps necessary to ensure that all those involved with the specified program or research project also abide by the provisions of this Agreement, and that the data received are not used for any purpose other than that specified in the *Application for Release of Restricted Data*.

This *Agreement* applies to all forms of personal communication, as well as to published results, presentations and reports.

The undersigned is authorized to execute this *Agreement*.

Principal Investigator, Program Director, or Other Responsible Individual:

Signature: _____ Date: _____

Printed Name and Title: _____

Organization: _____

Title of Program or Study:

_____

_____

Attachment 4

Employees' Confidentiality Statement

This Employee Confidentiality Statement is intended for use in at least the following two ways:

1. All employees must read and sign this Confidentiality Statement upon hire, and
2. This Confidentiality Statement must be reviewed and re-signed annually by all DHHS employees as part of the employee's annual performance evaluation, with the signed copy retained in the employee's personnel file.

Employees' Confidentiality Statement

This is to acknowledge that the Department of Health and Human Services, or its designee, has explained the following to me:

I am signing this form to acknowledge that the Department of Health and Human Services, or its designee, has explained to me the necessity of and legal requirement to keep client information confidential and to make sure that my access to confidential information is restricted to that whatever is needed to perform my job-related tasks. I have received training about confidentiality, and I acknowledge that I am responsible for knowing what information is by law, statute and rule required to be held confidentially. I am responsible for knowing what confidential information is necessary for me to perform my job-related tasks here in the department. By signing this form, I agree to meet the requirements of those laws at all times during and after my employment, for as long as I hold or have access to any confidential information.

This information may be related to any individual receiving services from or through any program administered or funded by any entity of the Department of Health & Human Services.

I understand that seeking, obtaining, receiving, retrieval or dissemination by me of any such information, whether retrieved or derived from paper or computer sources or in any other manner, except in the course of and for the purposes of performing my duties, is expressly prohibited.

In the situation where I inadvertently discover confidential information in client records, either paper or computer or any other manner, concerning individuals to whom I am related or have a personal relationship, I shall immediately terminate my access to this information. I will make my supervisor aware of the incident of inadvertent access.

If I have any questions regarding any aspect of confidentiality, I understand that I should consult my supervisor.

Please Note: FAILURE TO ADHERE TO THE CONFIDENTIALITY PROVISIONS OF STATE LAW MAY RESULT IN DISCIPLINARY ACTION UP TO AND INCLUDING TERMINATION.

I understand that the unauthorized disclosure of confidential information may also result in civil or criminal penalties as set out in law.

Date	Employee
Witness	Witness's Printed Name

Distribution: Original:.....Return to Personnel for employee's personnel file.
Copy:.....Employee
Copy:.....Supervisor's fact file

Attachment 5

Model Document 3: Only for programs deemed HIPAA "Covered Entities"

Maine Center for Disease Control and Prevention
Department of Health and Human Services

Summary Notice of Privacy Practices

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.

In compliance with the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Maine CDC, (Program Name) safeguards the Protected Health Information (PHI) of Clients whose Individually Identifiable Health Information is maintained in our records. As a client of (Program Name) , you have the right to expect that only those individuals, organizations and/or agencies that have a need to know will be granted permission to use your PHI, unless otherwise allowed by law or by your written authorization. Below is a brief description of your rights to privacy. These rights are explained more thoroughly in the pages that follow.

Disclosure of Protected Health Information –

Request for Privacy Protection for PHI –

Request for Restrictions on Disclosure of PHI –

Request for Confidential Communications of Protected Health Information –

Your Right to Inspect and Copy Protected Health Information –

Denial of Access –

Amendment of Protected Health Information –

Accounting of Disclosures –

Uses and Disclosures of Protected Health Information Requiring You to Agree or Object –

Uses and Disclosures of Protected Health Information Regarding Deceased Individuals –

Complaint Process –

Notice of Privacy Practices

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.

In compliance with the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Maine CDC, (Program Name), safeguards the Protected Health Information (PHI) of Clients whose Individually Identifiable Health Information is maintained in our records. As a Client of (Program Name), you have the right to expect that only those individuals, organizations and/or agencies that have a need to know will be granted permission to use your PHI, unless otherwise allowed by law or by your written authorization.

Disclosure of Protected Health Information

When Maine CDC discloses your PHI, the information that is disclosed will not:

- Exceed what is requested in a Medical Authorization; or
- Exceed what is reasonably required for the purpose for which it was disclosed, subject to the professional judgment of Maine CDC staff. Maine CDC reserves the right to determine whether or not the PHI requested **exceeds** the minimum necessary and to limit the PHI disclosed as appropriate.

Request for Privacy Protection for PHI

You may request that the use or disclosure of your PHI be restricted; however, Maine CDC is not required to agree with these restrictions. If we do agree to restrict disclosure of your PHI, these restrictions will be documented, and we will retain this documentation for six (6) years.

Request for Restrictions on Disclosure of PHI

You may request that the use or disclosure of PHI for other than Treatment, Payment or Health Care Operations be restricted; however, Maine CDC is not required to agree to those restrictions. If we do agree to a restriction, it will be honored. Additionally,

- If Maine CDC terminates the restriction, it will only be terminated after you have been informed in writing.
- If you terminate the restriction, then the PHI will be used and disclosed as otherwise permitted by law.
- If there is an emergency situation, information may be released to appropriate health care providers. These health care providers will be requested not to further use or disclose the information.

Request for Confidential Communications of Protected Health Information

All reasonable requests for confidential communication of PHI will be honored provided that you clearly state that you could be endangered by the disclosure of all or part of the PHI. Additionally, you must provide us with an alternative address or method of contact; otherwise, Maine CDC may refuse to accommodate your request.

Your Right to Inspect and Copy Protected Health Information

You have the right to inspect and obtain a copy of certain PHI maintained in Maine CDC files. Generally, the following material is maintained by Maine CDC, although individual Clients' files may not include all this material:

- Prior authorization files
- Medical eligibility assessments

Denial of Access

If you are denied access to your PHI, you may file a complaint with the Maine CDC Privacy Officer, the DHHS Deputy Commissioner, or the Secretary of Health and Human Services. Information on how to contact these offices is listed under *Complaint Process* at the end of this Notice.

Amendment of Protected Health Information

You have the right to amend your PHI or other records maintained in certain Maine CDC files for as long as that PHI is maintained in our files. Please see *Your Right to Inspect and Copy Protected Health Information,* above, for a list of the material maintained by Maine CDC.

Your request to amend PHI may be denied if it is determined that the material in question:

- Was not created by Maine CDC, unless the original source of the information is no longer available to make the requested corrections;
- Is not part of the files listed above;
- Is not available for inspection (see *Your Right to Inspect and Copy Protected Health Information*, above); or
- Is currently accurate and complete.

Accounting of Disclosures

You have the right to request an accounting of all disclosures of your PHI that Maine CDC may make, if the disclosure was for something other than Treatment, Payment or Health Care Operations, or as authorized by you.

Uses and Disclosures of Protected Health Information Requiring You to Agree or Object

When PHI is made available to the following groups, (Program Name) will give you the opportunity to object if you are capable of making health care decisions and the situation is not an emergency:

Health care institutions or directors involved in your health care;
Family members, close friends, or other persons assisting in your health care; or
Government agencies and disaster relief organizations involved in disaster relief efforts.

Uses and Disclosures of Protected Health Information Regarding Deceased Individuals

The HIPAA Privacy Rule safeguards PHI about deceased individuals for as long as that information is maintained in Maine CDC files. An executor, administrator, trustee, or other person who has authority to act on behalf of a deceased individual will be treated as a personal representative with respect to PHI. A deceased individual's PHI will be protected in the same manner and to the same extent as that of other individuals, except for uses and disclosures for research purposes.

Complaint Process

If you believe your Protected Health Information has not been safeguarded properly, you have the right to file a complaint either directly with Maine CDC or with the Secretary of Health and Human Services.

The Maine CDC Privacy Officer is responsible for receiving complaints regarding Privacy practices. You may reach the Privacy Officer by calling 207-287-3266

You may also file a complaint with the Secretary of Health and Human Services by calling, toll free, 1-877-696-6775 or writing to the Secretary at 200 Independence Avenue SW, Washington, D.C. 20201. Or, you may file a grievance with the Office of Civil Rights by calling, toll free, 1-866-OCR-PRIV (866-627-7748) or 1-886-788-4989 TTY.

Maine CDC documents all complaints. While we are not obligated to respond to all complaints, we do retain a copy of all complaint documents for six (6) years.

It is the strict policy of Maine CDC that there will be no retribution or retaliation against anyone filing a complaint against Maine CDC or a member of its staff.

1. A complaint must be filed in writing, either on paper or electronically.
2. A complaint must name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.
3. A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless the time limit is waived by the Secretary for good cause shown.

Attachment 6: Data Inventory

Please complete a separate survey form for each data collection system in your program

A. Program Information

1. Person completing this survey:

Name: _____ Office phone: _____

2. Division:

- ☐ Administration
- ☐ Environmental Health
- ☐ Infectious Disease
- ☐ Public Health Systems
- ☐ Chronic Disease
- ☐ Family Health

3. Program: _____

B. Data Collection Systems

1. Name of data collection system: _____

2. Storage method:

- ☐ Electronic (software used _____)
- ☐ Paper-based

3. Is this data collection system a surveillance system?

☐ Yes (go to QUESTION 3a.) ☐ No (go to QUESTION 4.)

3a. ☐ Active and/or ☐ Passive

3b. ☐ Population-based -- full population coverage

☐ Population-based -- based on a sample
Please describe the sampling scheme: _____

☐ Sentinel
Please describe the selection of sentinel sites for this surveillance system:

_____

4. Is this data collection system service-based?

☐ Yes (go to QUESTION 4a) ☐ No (Go to QUESTION 5)

4a. On whom is data collected? (e.g. all Medicaid patients)

_____

4b. What triggers data collection? (e.g. receipt of service)

_____

5. Please provide a brief summary of the data collection system (eg. The information collected, type of routine reports, etc)

Attachment 7: Data Use Plan

A. Program Information

1. Person completing this survey:

Name: _____ Office phone: _____

2. Division:

- ☐ Administration
- ☐ Environmental Health
- ☐ Infectious Disease
- ☐ Public Health Systems
- ☐ Chronic Disease
- ☐ Family Health

3. Program: _____

B. Secondary Data Use

Does your program use data collected by other Maine CDC programs?

☐ No: You've finished completing this form. *Thank you.*

☐ Yes: Please use the spaces below to list the *all* data used, the program that collects it, and the frequency of use. This includes data used for: analysis; planning; evaluation; program management; and response to outbreaks, bioterrorism or public health emergencies. Use reverse of form if needed)

Data Used	Program responsible for primary collection	Purpose of use	Data disseminated outside your program? (Yes/No)	Frequency of use (i.e. weekly, monthly, annually, sporadic)
1.				
2.				
3.				
4				
5.				